

1/11

Fig. 1

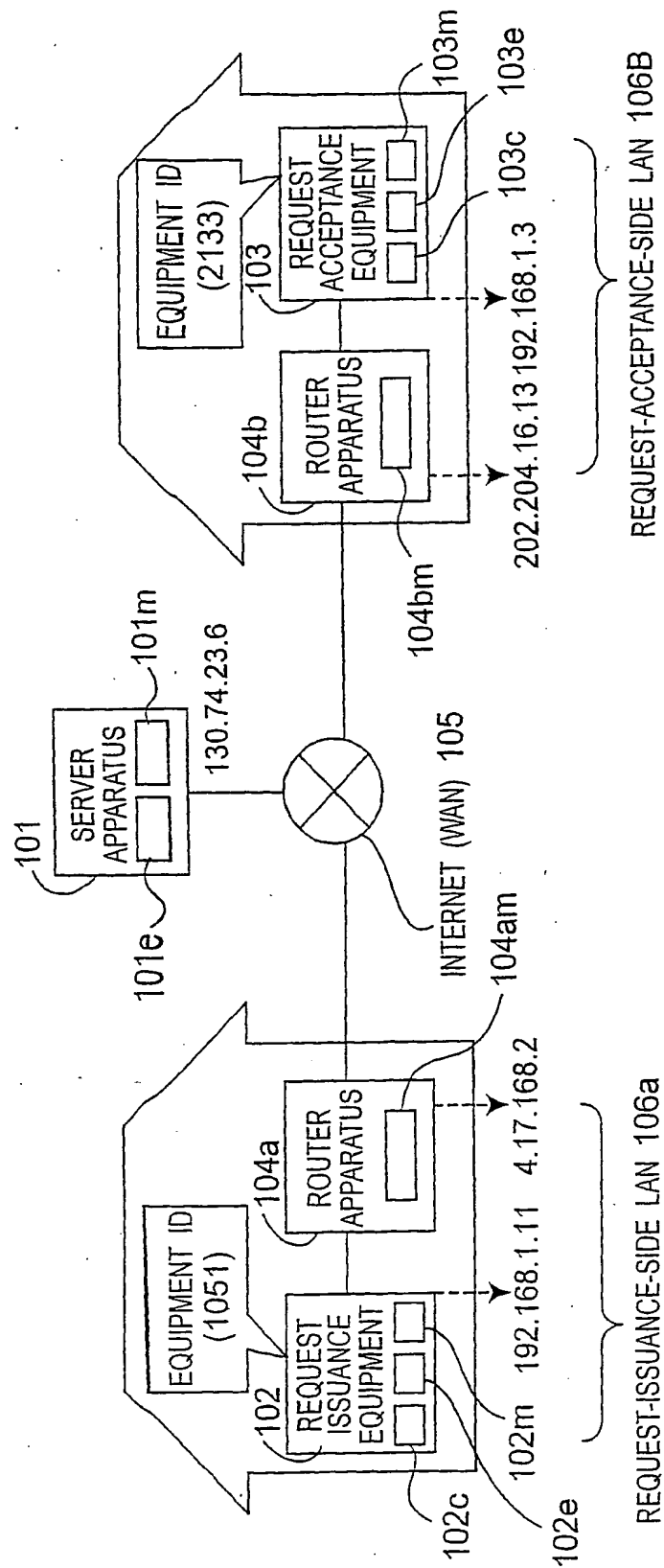


Fig. 2

2/11

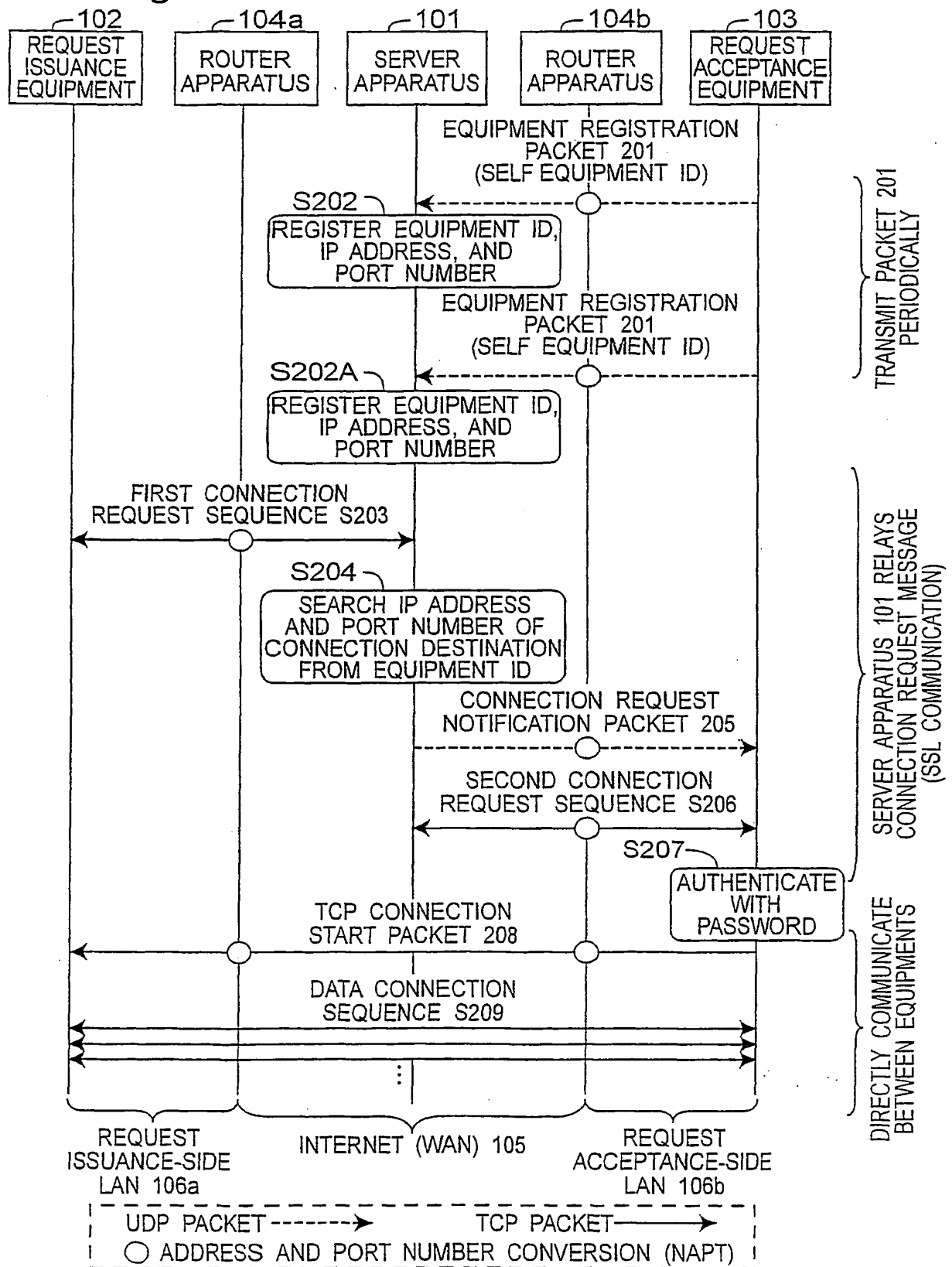
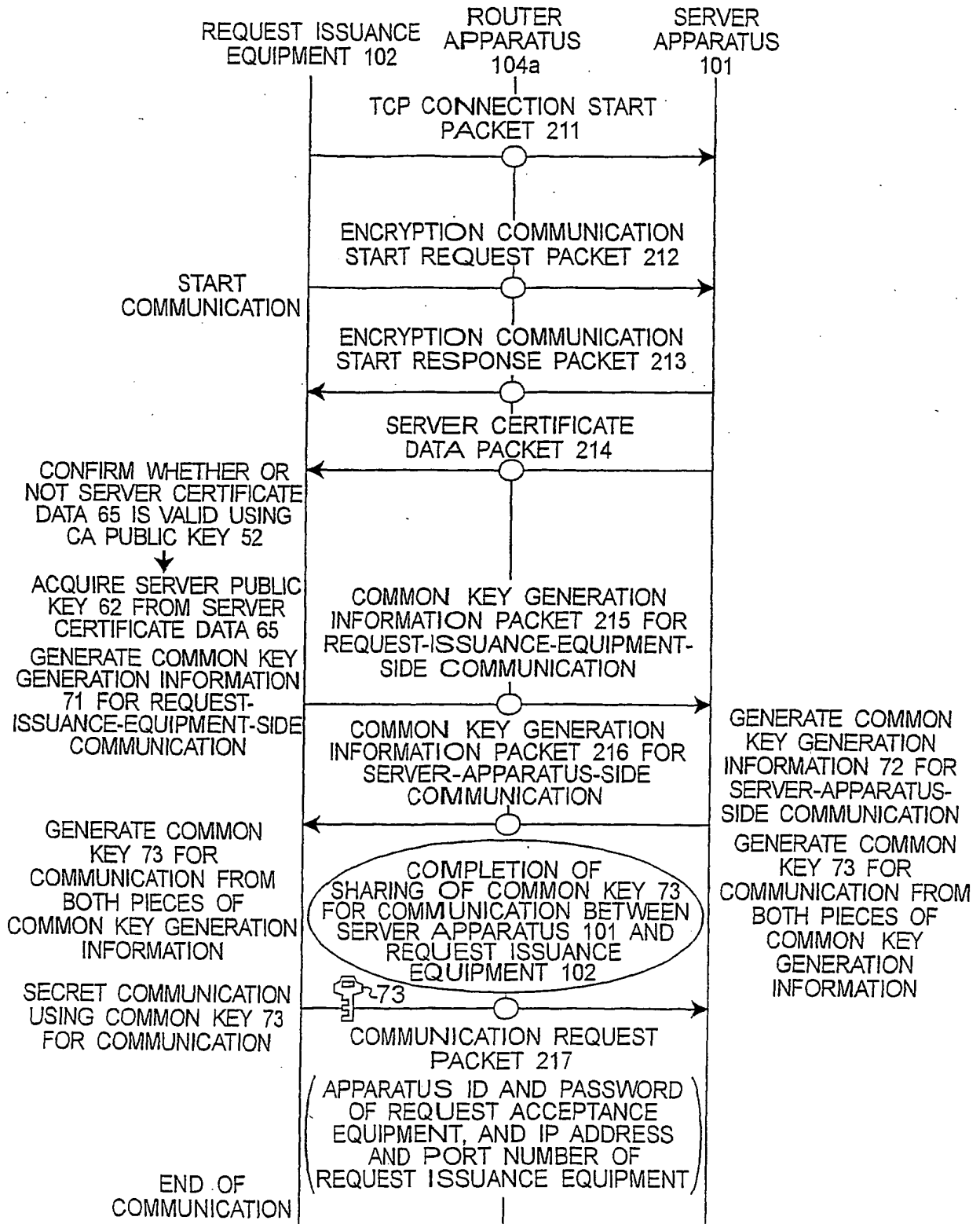


Fig. 3

3/11

## FIRST CONNECTION REQUEST SEQUENCE S203



```

sequenceDiagram
    participant S as SERVER APPARATUS 101
    participant R as ROUTER APPARATUS 104b
    participant A as REQUEST ACCEPTANCE EQUIPMENT 103

    S->>R: TCP CONNECTION START PACKET 221
    R->>S: ENCRYPTION COMMUNICATION START REQUEST PACKET 222
    R->>S: ENCRYPTION COMMUNICATION START RESPONSE PACKET 223
    S->>A: SERVER CERTIFICATE DATA PACKET 214
    Note over A: CONFIRM WHETHER OR NOT SERVER CERTIFICATE DATA 65 IS VALID USING CA PUBLIC KEY 52
    Note over A: ACQUIRE SERVER PUBLIC KEY 62 FROM SERVER CERTIFICATE DATA 65
    Note over A: GENERATE COMMON KEY GENERATION INFORMATION 81 FOR REQUEST-ACCEPTANCE-EQUIPMENT-SIDE COMMUNICATION
    R->>S: COMMON KEY GENERATION INFORMATION PACKET 224 FOR REQUEST-ACCEPTANCE-EQUIPMENT-SIDE COMMUNICATION
    Note over S: GENERATE COMMON KEY GENERATION INFORMATION 82 FOR SERVER-APPARATUS-SIDE COMMUNICATION
    Note over S: GENERATE COMMON KEY 83 FOR COMMUNICATION FROM BOTH PIECES OF COMMON KEY GENERATION INFORMATION
    S->>A: COMMON KEY GENERATION INFORMATION PACKET 225 FOR SERVER-APPARATUS-SIDE COMMUNICATION
    Note over A: GENERATE COMMON KEY 83 FOR COMMUNICATION FROM BOTH PIECES OF COMMON KEY GENERATION INFORMATION
    Note over S, R, A: COMPLETION OF SHARING OF COMMON KEY 83 FOR COMMUNICATION BETWEEN SERVER APPARATUS 101 AND REQUEST ACCEPTANCE EQUIPMENT 103
    S->>A: CONNECTION REQUEST PACKET 226 (PASSWORD, AND IP ADDRESS AND PORT NUMBER OF REQUEST ISSUANCE EQUIPMENT)
    Note over S: SECRET COMMUNICATION USING COMMON KEY 73 FOR COMMUNICATION
    Note over S: END OF COMMUNICATION
  
```

The diagram illustrates the communication process between three entities: SERVER APPARATUS 101, ROUTER APPARATUS 104b, and REQUEST ACCEPTANCE EQUIPMENT 103. The process begins with a TCP connection start packet (221) from the server to the router. The router then sends an encryption communication start request packet (222) to the server, which responds with an encryption communication start response packet (223). The server then sends a server certificate data packet (214) to the request acceptance equipment. The request acceptance equipment confirms the validity of the server certificate data (65) using the CA public key (52) and acquires the server public key (62) from the server certificate data (65). It then generates common key generation information (81) for request-acceptance-equipment-side communication. The router sends a common key generation information packet (224) to the server. The server generates common key generation information (82) for server-apparatus-side communication and generates a common key (83) for communication from both pieces of common key generation information. The server then sends a common key generation information packet (225) to the request acceptance equipment. The request acceptance equipment generates a common key (83) for communication from both pieces of common key generation information. The process then completes the sharing of the common key (83) for communication between the server apparatus (101) and the request acceptance equipment (103). The server then sends a connection request packet (226) to the request acceptance equipment, which includes a password, IP address, and port number of the request issuance equipment. The server also performs secret communication using the common key (73) for communication. The process ends with the end of communication.

5/11

Fig.5

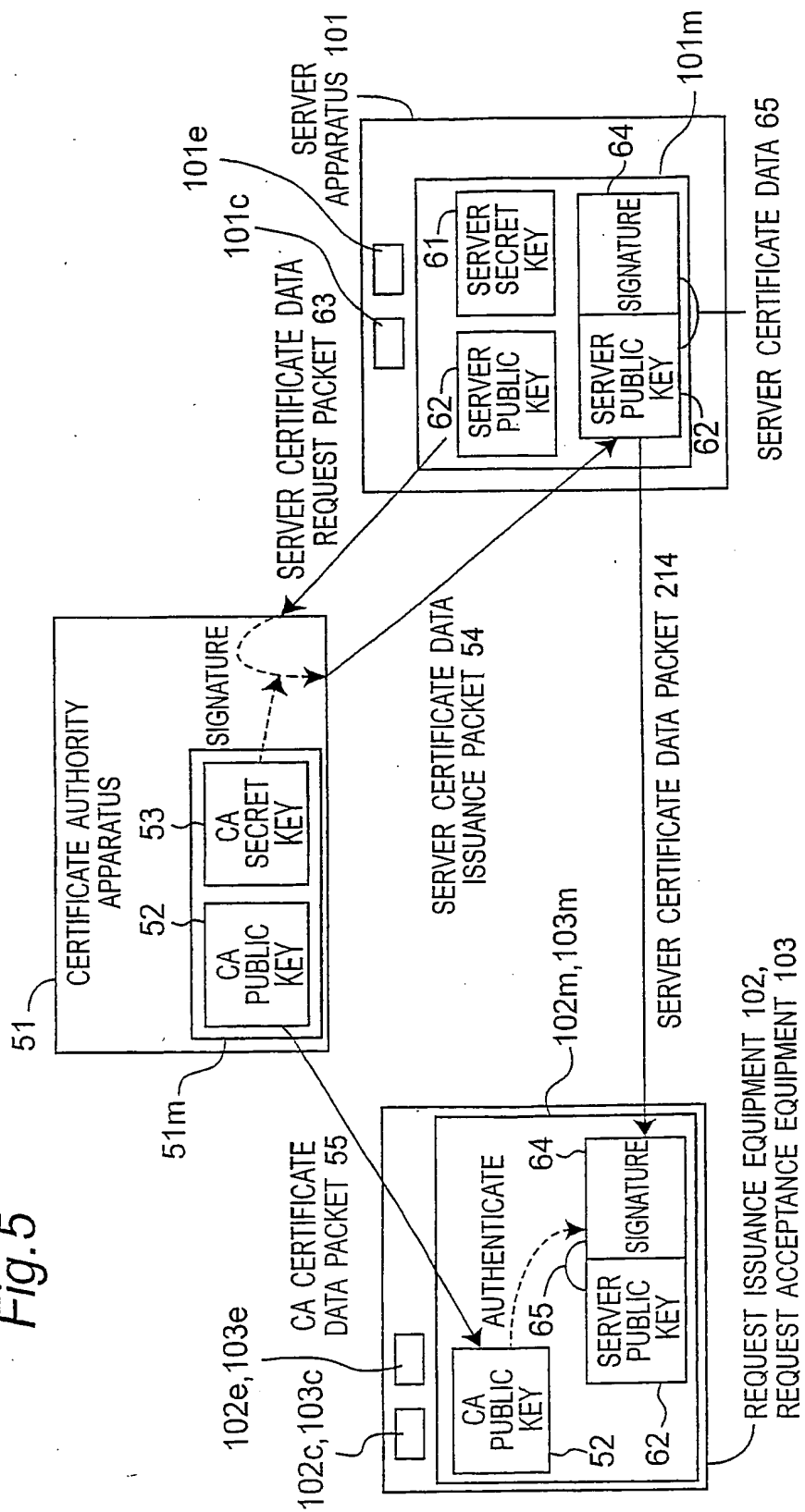


Fig.6

104am

LAN EQUIPMENT ADDRESS	WAN ROUTER ADDRESS	LAN EQUIPMENT PORT NUMBER	WAN ROUTER PORT NUMBER	
192.168.1.11	4.17.168.2	1500	7000	FOR TCP COMMUNICATION WITH SERVER APPARATUS 101
192.168.1.11	4.17.168.2	1600	5000	FOR TCP COMMUNICATION WITH REQUEST ACCEPTANCE EQUIPMENT 103
---	---	---	---	

*Fig. 7A*EQUIPMENT REGISTRATION  
PACKET 201 (LAN SIDE)

SA= 192.168.1.3
DA= 130.74.23.6
SP= 2000
DP= 1200
EQUIPMENT ID OF REQUEST ACCEPTANCE EQUIPMENT 103 (2133)

SA: SOURCE ADDRESS FIELD  
 DA: DESTINATION ADDRESS FIELD  
 SP: SOURCE PORT NUMBER FIELD  
 DP: DESTINATION PORT NUMBER FIELD

*Fig. 7B*EQUIPMENT REGISTRATION  
PACKET 201 (WAN SIDE)

SA= 202.204.16.13
DA= 130.74.23.6
SP= 3400
DP= 1200
EQUIPMENT ID OF REQUEST ACCEPTANCE EQUIPMENT 103 (2133)

SA: SOURCE ADDRESS FIELD  
 DA: DESTINATION ADDRESS FIELD  
 SP: SOURCE PORT NUMBER FIELD  
 DP: DESTINATION PORT NUMBER FIELD

*Fig. 7C*CONNECTION REQUEST  
PACKET 217 (LAN SIDE)

SA= 192.168.1.11
DA= 130.74.23.6
SP= 1500
DP= 1201
EQUIPMENT ID OF REQUEST ACCEPTANCE EQUIPMENT 103 (2133)
PASSWORD OF REQUEST ACCEPTANCE EQUIPMENT 103
IP ADDRESS OF REQUEST- ISSUANCE-SIDE LAN 106a (4.17.168.2)
PORT NUMBER OF REQUEST- ISSUANCE-SIDE LAN 106a (5000)

SA: SOURCE ADDRESS FIELD  
 DA: DESTINATION ADDRESS FIELD  
 SP: SOURCE PORT NUMBER FIELD  
 DP: DESTINATION PORT NUMBER FIELD

*Fig. 7D*CONNECTION REQUEST  
PACKET 217 (WAN SIDE)

SA= 4.17.168.2
DA= 130.74.23.6
SP= 7000
DP= 1201
EQUIPMENT ID OF REQUEST ACCEPTANCE EQUIPMENT 103 (2133)
PASSWORD OF REQUEST ACCEPTANCE EQUIPMENT 103
IP ADDRESS OF REQUEST- ISSUANCE-SIDE LAN 106a (4.17.168.2)
PORT NUMBER OF REQUEST- ISSUANCE-SIDE LAN 106a (5000)

SA: SOURCE ADDRESS FIELD  
 DA: DESTINATION ADDRESS FIELD  
 SP: SOURCE PORT NUMBER FIELD  
 DP: DESTINATION PORT NUMBER FIELD

*Fig. 8A*

CONNECTION REQUEST NOTIFICATION  
PACKET 205 (LAN SIDE)

SA= 130.74.23.6
DA= 192.168.1.3
SP= 1200
DP= 2000
CONNECTION REQUEST NOTIFICATION FLAG

SA: SOURCE ADDRESS FIELD  
DA: DESTINATION ADDRESS FIELD  
SP: SOURCE PORT NUMBER FIELD  
DP: DESTINATION PORT NUMBER FIELD

*Fig. 8B*

CONNECTION REQUEST NOTIFICATION  
PACKET 205 (WAN SIDE)

SA= 130.74.23.6
DA= 202.204.16.13
SP= 1200
DP= 2400
CONNECTION REQUEST NOTIFICATION FLAG

SA: SOURCE ADDRESS FIELD  
DA: DESTINATION ADDRESS FIELD  
SP: SOURCE PORT NUMBER FIELD  
DP: DESTINATION PORT NUMBER FIELD

*Fig. 8C*

CONNECTION REQUEST  
PACKET 226 (LAN SIDE)

SA= 130.74.23.6
DA= 192.168.1.3
SP= 1300
DP= 2600
PASSWORD OF REQUEST ACCEPTANCE EQUIPMENT 103
IP ADDRESS OF REQUEST- ISSUANCE-SIDE LAN 106a (4.17.168.2)
PORT NUMBER OF REQUEST- ISSUANCE-SIDE LAN 106a (5000)

SA: SOURCE ADDRESS FIELD  
DA: DESTINATION ADDRESS FIELD  
SP: SOURCE PORT NUMBER FIELD  
DP: DESTINATION PORT NUMBER FIELD

*Fig. 8D*

CONNECTION REQUEST  
PACKET 226 (WAN SIDE)

SA= 130.74.23.6
DA= 202.204.16.13
SP= 1300
DP= 2401
PASSWORD OF REQUEST ACCEPTANCE EQUIPMENT 103
IP ADDRESS OF REQUEST- ISSUANCE-SIDE LAN 106a (4.17.168.2)
PORT NUMBER OF REQUEST- ISSUANCE-SIDE LAN 106a (5000)

SA: SOURCE ADDRESS FIELD  
DA: DESTINATION ADDRESS FIELD  
SP: SOURCE PORT NUMBER FIELD  
DP: DESTINATION PORT NUMBER FIELD

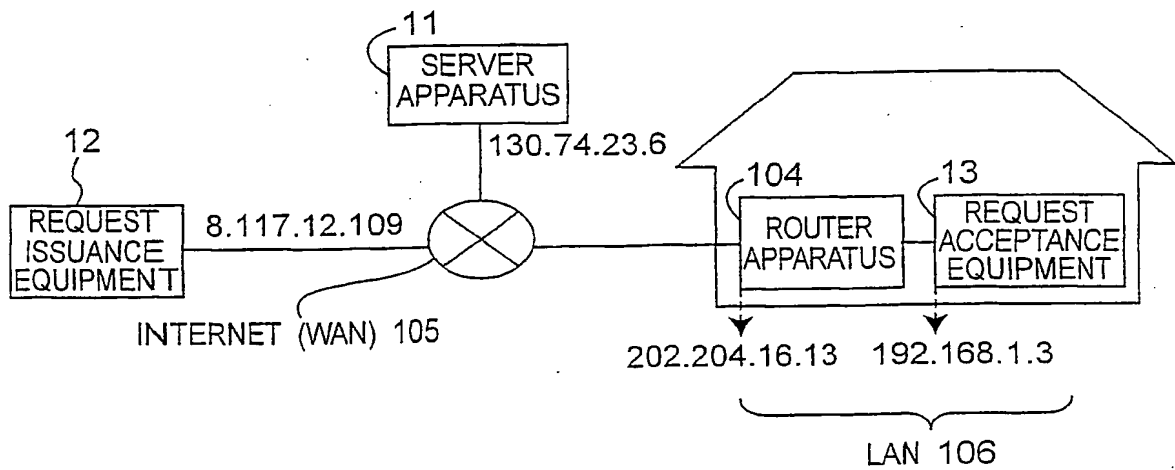


Fig.9

101m  
↙

EQUIPMENT ID	IP ADDRESS	PORT NUMBER
2133	202.204.16.13	3400
---	---	---
---	---	---

Fig.10



10/11

Fig. 11

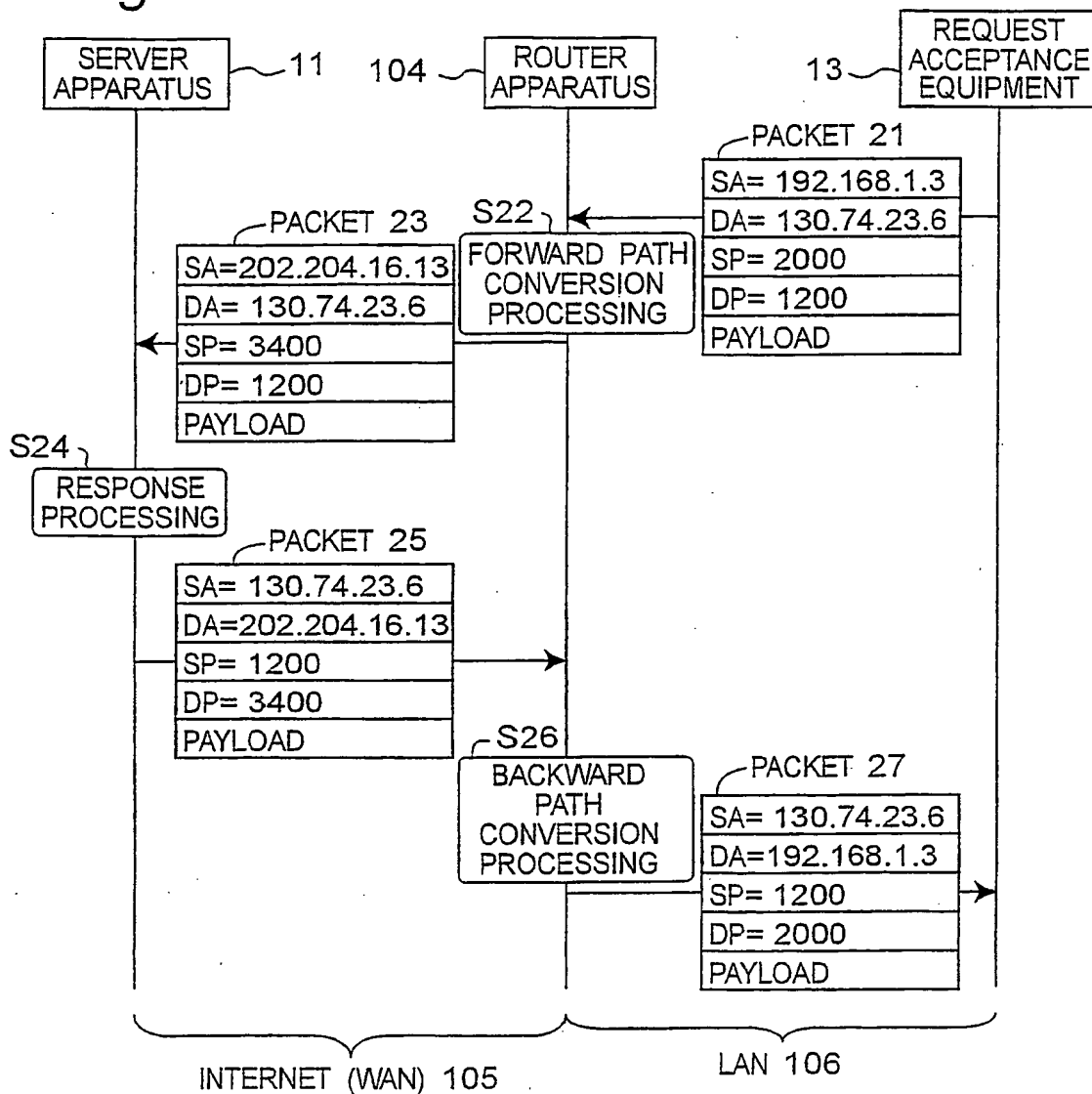


Fig. 12

LAN EQUIPMENT ADDRESS	WAN ROUTER ADDRESS	LAN EQUIPMENT PORT NUMBER	WAN ROUTER PORT NUMBER
192.168.1.3	202.204.16.13	2000	3400
---	---	---	---
---	---	---	---

Fig. 13

